MyProxy Online Credential Repository

Jim Basney <jbasney@ncsa.uiuc.edu>, National Center for Supercomputing Applications, University of Illinois

What is MyProxy?

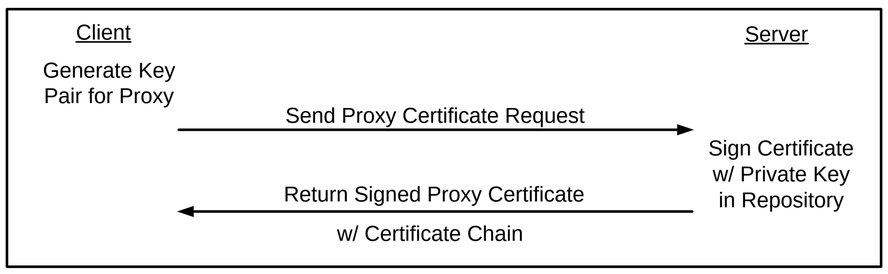
MyProxy is a credential repository for the Grid. Storing Grid credentials in a MyProxy repository allows users to retrieve a credential whenever and wherever they need one, without needing to manage private key and certificate files.

Why use MyProxy?

Improved Usability: Users obtain a Grid credential by running a single command and entering their passphrase from any machine on the Grid where a MyProxy client is installed.
Improved Security: Long-term credentials need not be copied to many machines on the Grid. Instead, short-term proxy credentials are retrieved on demand from the MyProxy repository. The MyProxy repository provides a central point of control and audit for the credentials.
Flexibility: The MyProxy service can be deployed for a single user, a virtual organization, or a Certificate Authority. Credentials can be pre-loaded for the user or the user can store credentials only when needed.

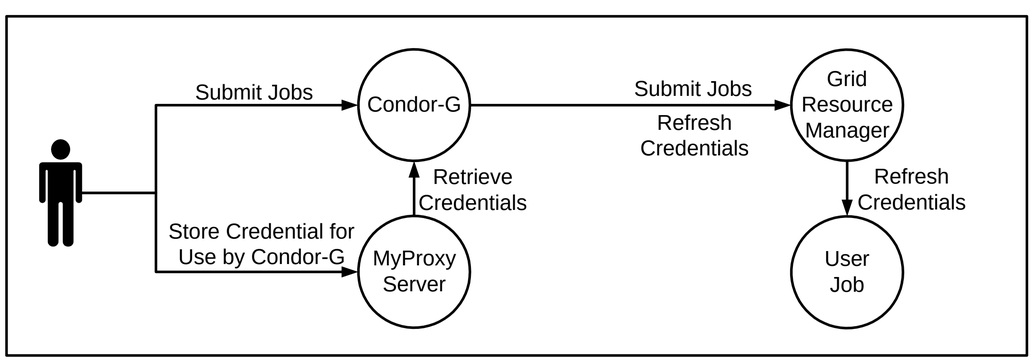
Proxy Delegation

MyProxy clients retrieve proxy credentials from the repository via delegation, so the private key in the repository is never sent over the network. The short lifetime of proxy credentials limits their exposure.



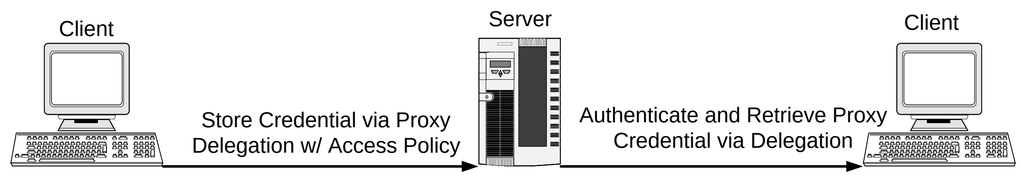
Credential Renewal with MyProxy

MyProxy supports credential renewal by allowing authorized services to renew a user's delegated credentials when needed before they expire, providing a trusted point of control and audit for the user's credentials in contrast to delegating long-lived credentials directly across the Grid.



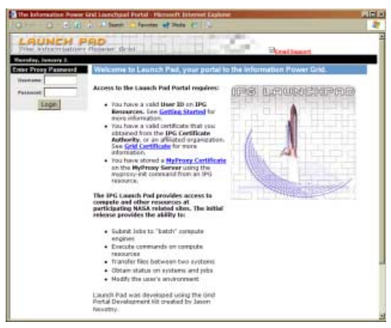
For example, a user can submit a long-running task to a job broker like Condor-G and authorize the broker to use MyProxy to renew credentials. If the job queues or runs longer than the lifetime of the credentials, the broker can authenticate to MyProxy and retrieve new credentials for the job, so the job can continue accessing Grid resources during its run.

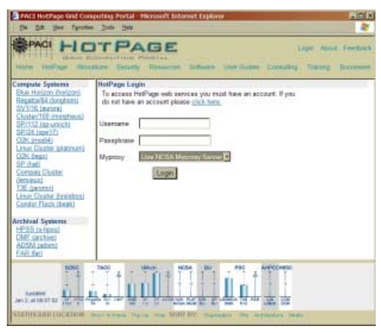
MyProxy Protocol Overview



MyProxy and Grid Portals

Grid Portals, which provide a standard Web interface to Grid services, require delegated credentials to act on the user's behalf. Standard web browsers don't support credential delegation, so MyProxy is used instead. The user stores a credential in the MyProxy repository and sends the username and passphrase to the portal (via https) under which it can retrieve the credentials from the repository.





Active Research and Development

Auditing: MyProxy will be integrated with a secure auditing service, providing query and notification interfaces for both users and administrators.
Authorization: Current ad-hoc access control mechanisms will be replaced by standards-based, extensible middleware authorization mechanisms.
Condor-G: MyProxy credential renewal will be integrated with Condor-G to provide unattended credential refresh for long-running jobs.
Kerberos: Support for Kerberos authentication and storing Kerberos tickets will provide the ability to translate between Kerberos and Grid (X.509) authentication tokens.
Multiple Credentials: Mechanisms will be developed to assist users in managing multiple credentials, including a negotiation mechanism to select the appropriate credentials for a task.
OGSA: MyProxy will be compliant with the emerging Open Grid Services Architecture with the specification and implementation of a MyProxy Grid Service.
Standardization: Protocols and APIs for credential management will be standardized in the Global Grid Forum.

Support and Acknowledgements

NSF Middleware Initiative
Information Power Grid
NASA's Computing and Data Grid
Alliance
NCSA
University of Illinois at Urbana-Champaign